inroads

Workbook

Holistic Security

for abortion stigma-busting work

Based on the training conducted by Kinga Jelinska and Ivette Mrova for the inroads community

OVERVIEW

- Introduction
- Discussion: What is security?
- What is holistic security?
- Threat modeling
- Activity: Risk assessment
- Creating a security plan
- Additional resources

WHO WE ARE

The International Network for the Reduction of Abortion Discrimination and Stigma (inroads) is a global network and community of practice dedicated to learning, skill-sharing, and making sustainable and measurable changes to reduce abortion stigma and its discriminatory outcomes locally and across the globe. We provide opportunities and resources to help learn, connect, collaborate, gather, and fund stigma-busting efforts worldwide

If you are not a member yet, join us today!
Membership is free.

What is security?

Security is a deeply personal, subjective and gendered concept.

In English, **safety** is the condition of being protected from, or unlikely to cause danger, risk, or injury.

Security is the state of being free from danger or threats.

In Spanish, **seguridad estar segura**, which can also mean being confident, being sure, or being safe.

Sentirse a salvo is to feel safe, with few or no risks.

Security Survey

1. Have you ever received a security training?

2. If so, what type of training was it?
(Eg. Holistic security, digital security, physical security, psychosocial security, other)

3. How impactful was the training that you had?

4. How confident do you feel about your security habits?

5. Are you concerned about your safety?

6. What are the risks and threats in relation to privacy and security that your organization faces?

7. Is there a person or persons in your group / organization who has knowledge of the various types of security, and takes a lead to implement them?

8. Are you familiar with risk assessment and do you regularly practice risk assessment as a part of your work?

Prompt: Amongst your group, based on your survey answers and personal/professional experiences, discuss what **security** means to you.

What is holistic security? (Part One)

Imagine having **very good digital security** in place, but **little to no well-being policies**.

-> Staff are stressed out, burning out, and more prone to NOT perceiving certain threats in the workplace, despite perhaps having strong digital security (the most commonly thought of, when one thinks of security in the workplace!)

There is an **ever-present risk** when people are too stressed or burnt out to **be able to contribute to the wellbeing AND the security** of the organization overall, **potentially impacting themselves and the people they work with.**

What is holistic security? (Part Two)

In this way, holistic security is about **integrating awareness and practices around security** – whether that's wellbeing, physical, or digital security – within all aspects of an individual and/or organization.

A **holistic security approach** is an approach to the security and protection of human rights defenders that recognizes the need for and promotes an **interdisciplinary understanding of systemic violence and the strategies needed to reduce it.**

Types of security

Physical security

The protection of the physical integrity of the organization and its members, including protection of the building, its hardware, and physical files and documentation. Travel and other forms of logistical security for events and workshops also fall under this category.

Digital and information security

The protection of online and offline data and infrastructure that could be exposed, such as websites, databases, servers and emails. Also, the protection of all channels of communication.

Self care and well-being

This involves the recognition of and strategies for the psychological and psychosocial impacts of the risks which members and consultants of human rights organizations face, related to the work that they carry out.

Holistic security

A holistic approach can also include legal and financial security, as well as other aspects of security that relate to the local and regional contexts in which organizations operate. It is important to recognize and integrate, to the extent possible, all these related aspects in the daily life, routines and response mechanisms of an organization.

Holistic security includes (among other things):

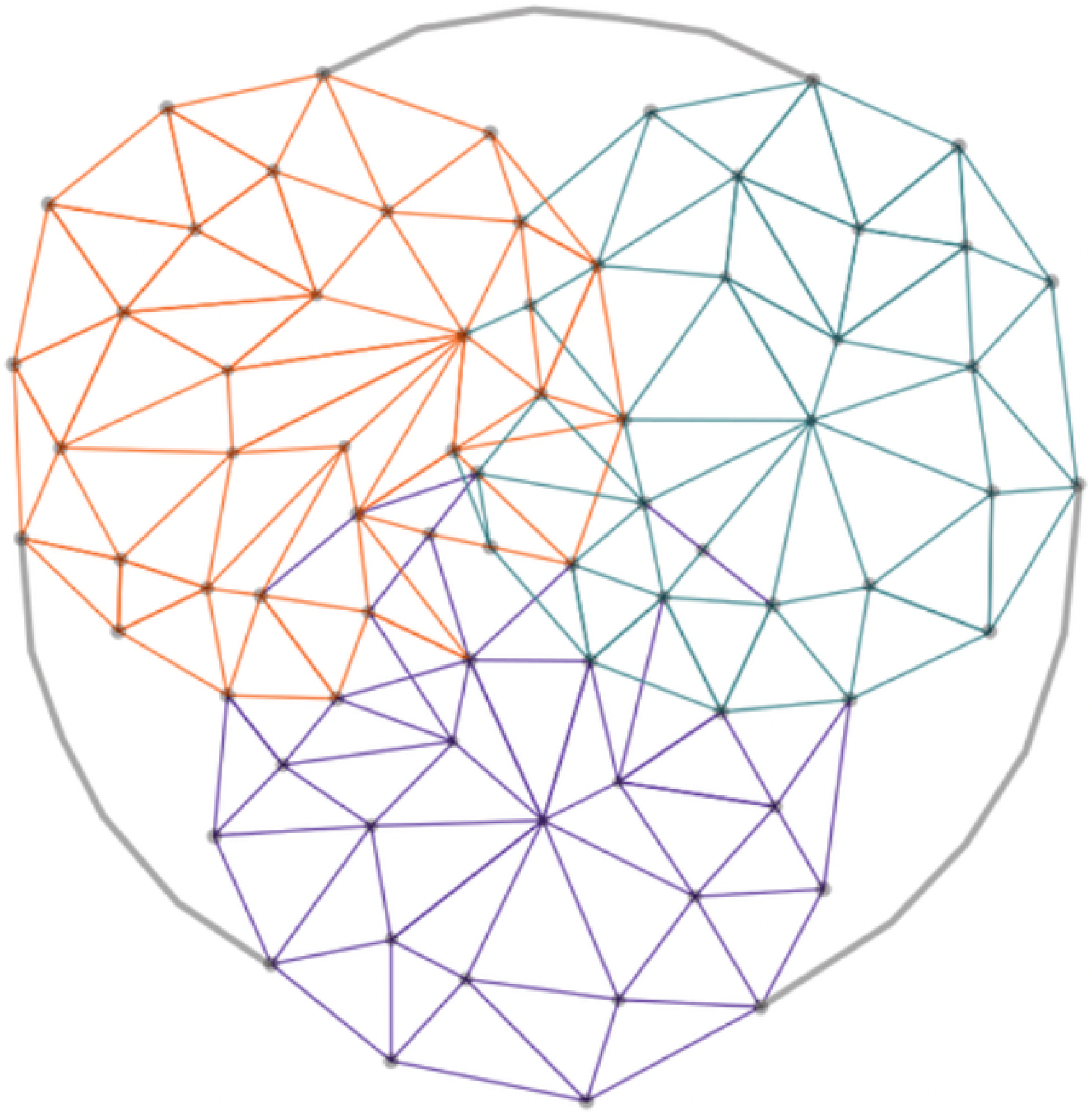
Holistic Security

△ **Physical Security**
Threats to our physical integrity. Threats to our homes, buildings, vehicles.

△ **Psycho-social Security**
Threats to our psychological wellbeing.

△ **Digital Security**
Threats to our information, comunication and equipment.

— Holistic security analysis, strategies and tactics.



Knowing your context

- **Reproductive justice** is based on the understanding that the negative impacts of class, gender, race and sexual identity are interwoven, creating a paradigm of **intersectionality**.

- Lack of access to abortion is linked to systemic marginalization, as disadvantaged communities often experience the **most challenges to reproductive health access**.

- Health, justice, and safety should **never be determined** by social, racial, or economic status.

What is a risk assessment?

We look both ways before crossing the street. As a child, you probably know (or learn!) not to put your hand to a flame, because if you do, you burn yourself.

We do this sort of risk assessment **our entire lives** without consciously realizing it.

The **physical aspect of risk** is something that most of us grow up being aware of.

Risk assessment

To understand the level of risk of an activity, it is necessary to measure the risk as high, medium, or low, **based on factors such as:**

- the identification of threats
- the assessment of the possibility of their occurrence
- the capacities we have to face them
- the impact they would have if they were carried out.

Risk assessments involve examining threats, vulnerabilities and capacities.

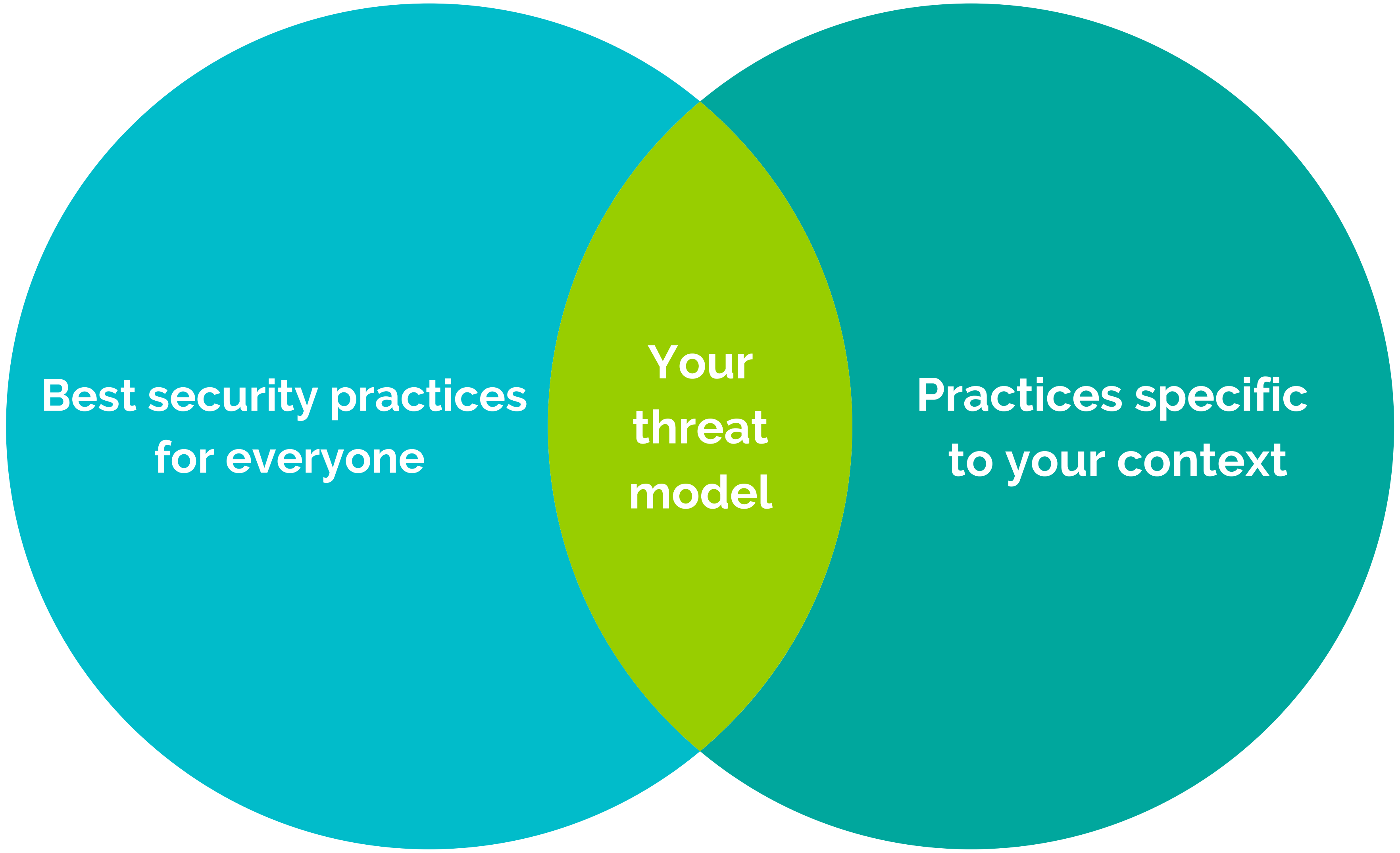
<u>The best way to predict what will happen is to look at what has already happened.</u>

What is a threat model?

A threat model consists of potential attacks against you, ranked by likelihood and severity.

It helps you overview and prioritize the security practices that will be most useful for you.

To identify the **best security practices** for your organization, you must first identify and know your specific context.



Best security practices for everyone

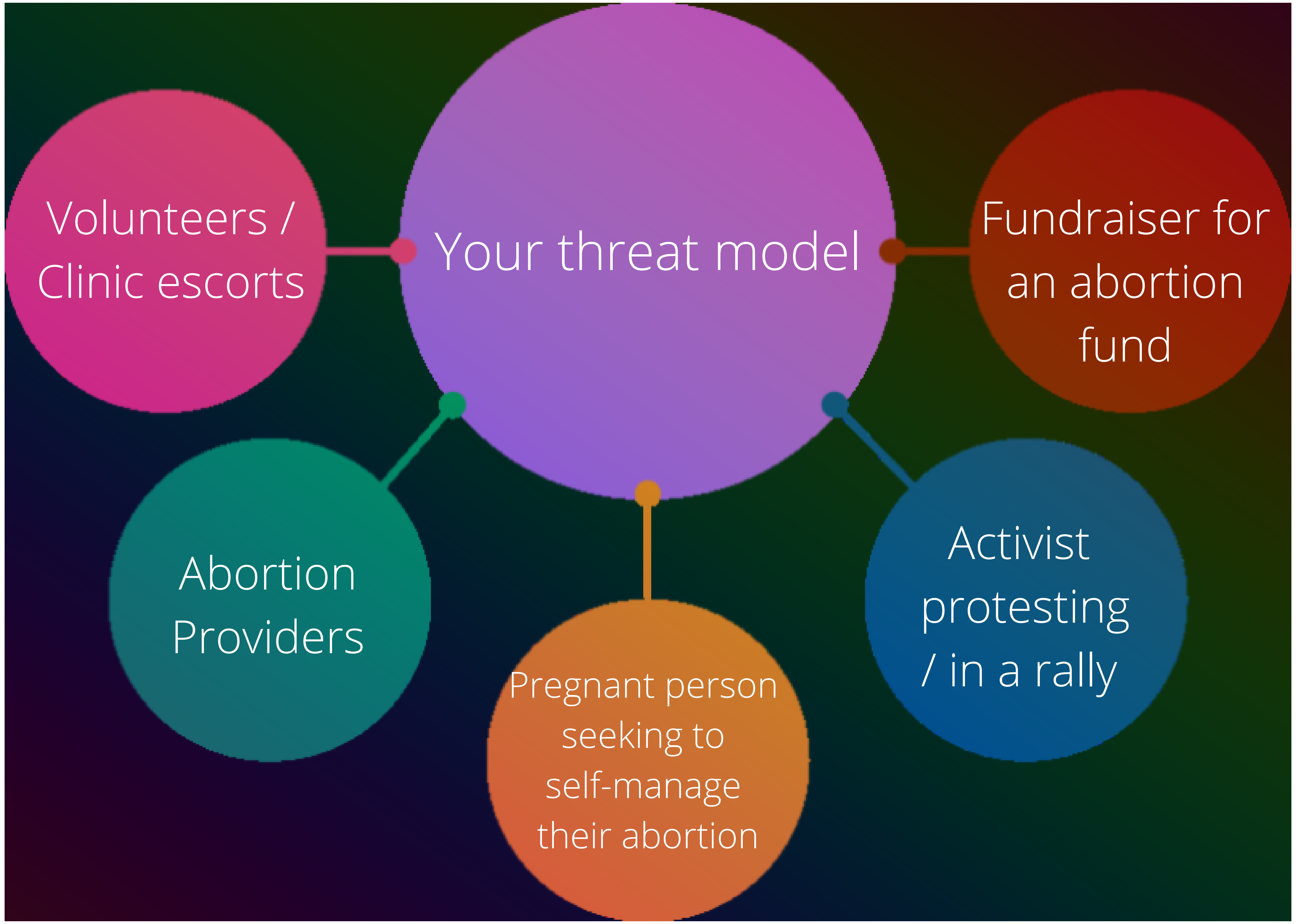
Your threat model

Practices specific to your context

Knowing your context:

Identify the type of work you are doing and the people you are doing it with/for will affect the type of threats you may face.

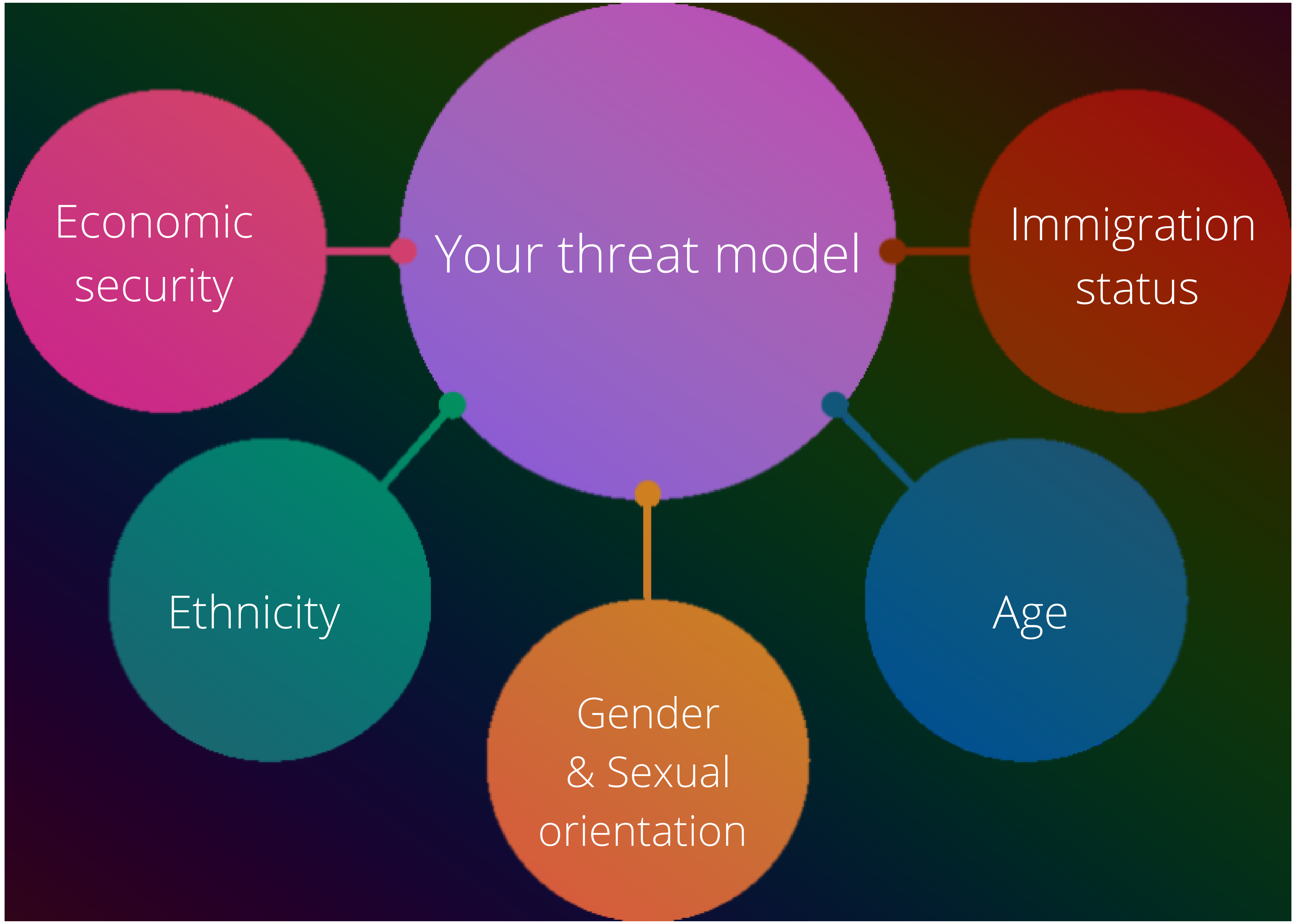
It should also guide your customized approach to a security plan, contingency plans, and others in your threat model.


Your threat model
Volunteers / Clinic escorts
Fundraiser for an abortion fund
Abortion Providers
Pregnant person seeking to self-manage their abortion
Activist protesting / in a rally

Knowing your context:

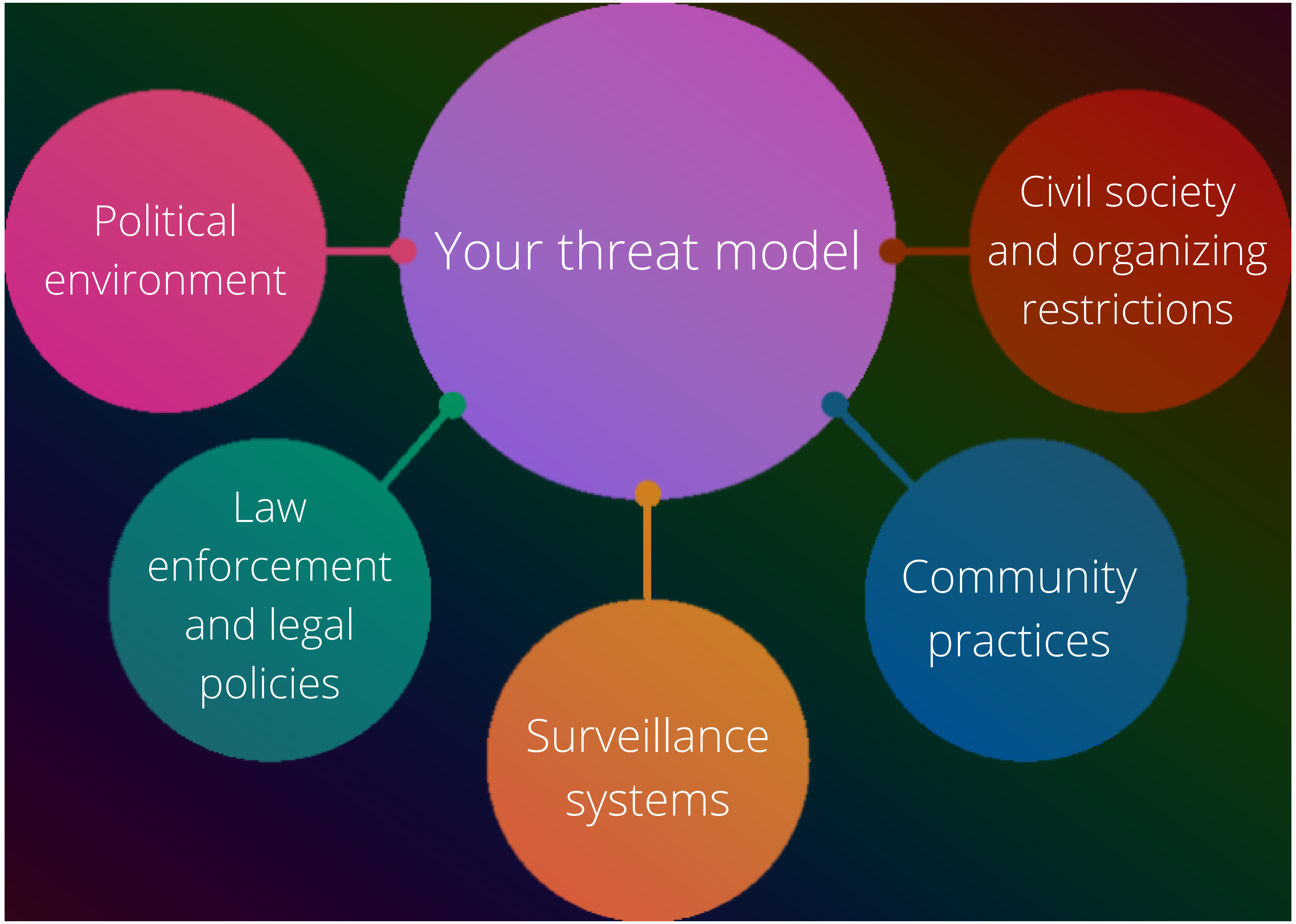
Important!

Take into consideration how your **identity** affects the way you are positioned in the world and how it may affect the severity of impact a threat might have --->



Knowing your context:

To understand your context and its various dimensions, you may also wish to analyze the following:



Definitions

Risk: Probable event or danger

Threat: Declaration or indication of an intention to inflict damage, punish, or hurt

Vulnerability: Open to attack or damage

Capacities: Available resources; the potential for holding, storing, or accommodating

Activity: Risk Assessment

Brainstorm and come up with a list of threats from different security domains relevant to your actions and work as a reproductive justice defender, using the risk assessment table in the following slide.

- Choose 2 to 3 threats that are important for your group and analyze them.
- Notice and pay attention to complexities.
- Estimate the level of risk (it can be different for each of you).

Risk Assessment Table

Threat	From who?	Why?	Existing Capacities	Required Capacities	Vulnerabilities	Risk Level

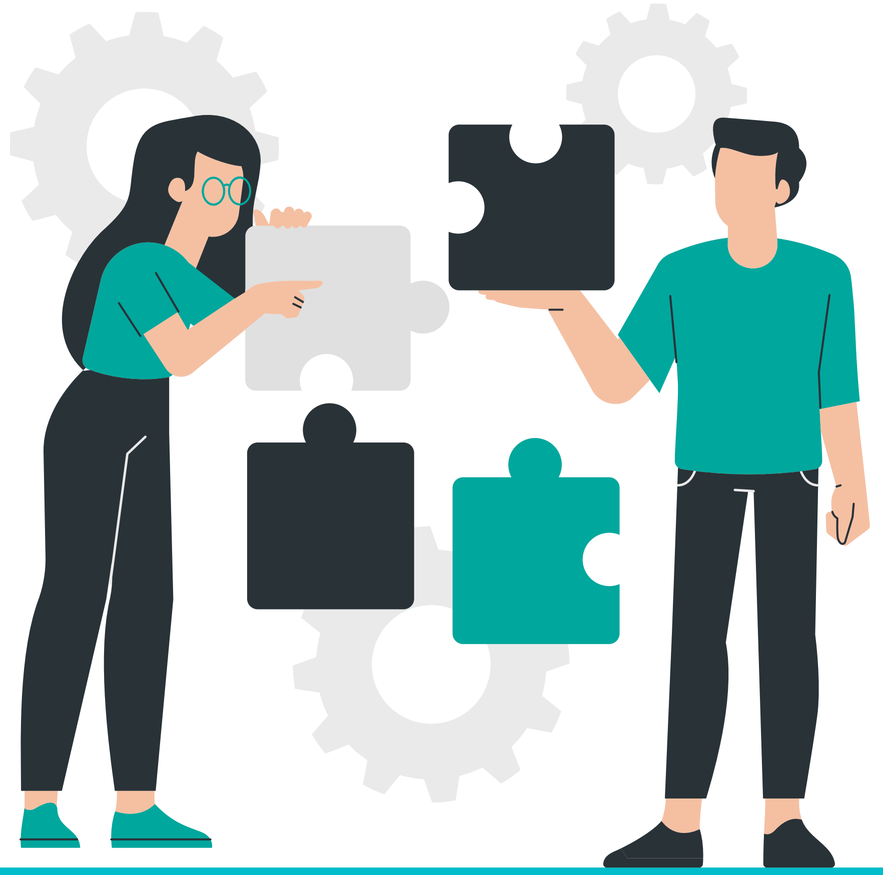
Risk Level Scale: 1 (very low), 2 (low), 3 (medium), 4 (high), 5 (very high)

Questions to include in your risk assessment:

- Have you and your group experienced any security incidents before?
- What is likely to occur?
- Are certain members of the group more visible/public?
- Are certain members of the group experiencing harassment or stalking?
- Are group members a part of marginalized communities?
- Who are the threat actors?
- What is the most important asset for you?
- What do you want to protect?
- Who do you want to protect it from?
- What are the tactics that you use or wish to use to protect it?
- What are the consequences if you fail?
- How likely are these consequences?
- How can you address the most likely risks?
- How the organisation can contribute?

Next Steps:

- Review your current security measures.
- Analyze your organizational infrastructure, policies, accounts, etc.
- Define your area of focus and priorities.
- Start with small steps.
- Start with key members with more public roles.
- Make it personal, then make it organizational.



Cultivate your security culture:

Establish your security baseline.

Build trust & get support from all members of your group.

Appoint a security person or team.

Explain the "why" with threat modeling.

Break the security plan up into smaller steps.

Practice account hygiene.

Build it into your existing practices.

Create a security plan:

Reduce the level of risk you are experiencing by:

- Identifying vulnerabilities.
- Using a risk assessment to plan next steps.
- Implementing a plan to reduce the vulnerabilities.
- Improving your capacities on at least three levels:
  - Individual
  - Organizational
  - Inter-organizational

Conclusion

Security is the **concern of all,** as it is individual, organizational, and inter-organizational.

Security is **complex** and is **the result of multiple, overlapping factors** in life.

Security plans should include day-to-day policies, preventative and preparatory measures, and specific situation protocols.

Resources

for cultivating your security culture

- Tips, tools, and techniques to keep you and your community safe while fighting for the right to reproductive healthcare: https://ssd.eff.org/en/playlist/reproductive-healthcare-service-provider-seeker-or-advocate

- RAWRR (Risk Assessment Workflow for Recommendation Roadmaps): https://conexo.org/project/rawrr/

- Free and simple tool that enables organizations to build better security policies: https://usesoap.app/

- Security guide for human rights defenders in Africa: https://www.defenddefenders.org/wp-content/uploads/2017/04/StandUp.pdf